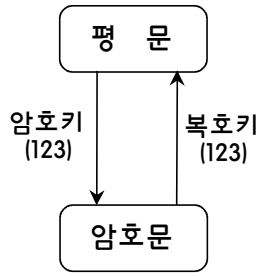
10. 암호(cipher)

암호는 **변형 기술**이다. 평문을 그 의미를 알 수 없는 암호문으로 변환하는 것이다.
암호화를 하면 정보가 해킹 등에 의해 비인가자에게 노출되어도 그 내용을 알 수 없게 된다.

// 암호 알고리즘 종류

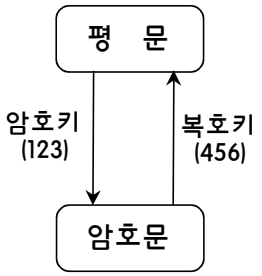
대칭키 암호	DES, SEED, AES, ARIA, HIGHT, IDEA, RC4, SkipJack
비대칭키 암호	RSA, Rabin, ElGamal, ECC, DSA, KCDSA, ECDSA **(공개키 암호)**
해시함수	MD5, HAS-160, SHA-1, SHA-2, WHIRLPOOL(월풀)

〈대칭키 암호〉



• 대칭키 암호 : 암호키 = 복호키

〈비대칭키 암호〉



• 비대칭키 암호 : 암호키 ≠ 복호키

• 암호화에서 암호키(비밀키)는 메시지를 열고 잠그는 상수(constant)이다.
• 암호학적 해시함수는 암호키를 사용하기도 하고, 사용하지 않기도 한다.(뒤에서 다룸)

[예제] 암호화 / 복호화를 단순하게 xor 연산만을 사용하는 경우 - 대칭키 원리

0101 ← 평문(메시지)
xor)1001 ← 키(암호키), 암호화 과정
1100 ← 암호문
xor)1001 ← 키(복호키), 복호화 과정
0101 ← 평문

◈ 암호 기본 원리

종 류	설 명
전치암호 (transposition cipher) (permutation cipher)	• 환치(換置) 암호라고도 한다. • 평문을 구성하는 문자 위치를 서로 바꿔 재배열 하는 방식 • 예 : 스키탈레 암호(scytale cipher)
대치암호 (substitution cipher)	• 환자(換字) 또는 치환암호라고도 한다. • 평문의 각 문자를 새로운 문자로 대치하는 방식 • 알파벳을 단순하게 이동시키는 방식으로 암호문을 생성 • 문자 치환표를 이용한 암호문을 생성 • 예 : 로마 황제 시저 암호(caesar cipher), 비지넬 암호
혼합암호 (product cipher)	• 전치암호와 치환암호를 혼합하는 방식 • 예 : 대칭키 암호인 DES, AES, SEED 등
대수적 암호 (algebraic cipher)	• 평문의 각 문자를 숫자로 바꾸어 수학적으로 처리 • 예 : 공개키 암호인 RSA, Rabin, ECC 등

◈ 대칭키 암호 용어 정리 및 사용상 주의할 점

"전치 / 순열 / 대치" 용어의 관계를 정확하게 숙지하도록 한다.

한국어	영 어	의 미
전치	transposition	• 평문을 구성하는 **문자 위치를 서로 바꿔 재배열** 하는 방식 • 환치(換置)라고도 한다. • 예 : 123 → 312
순열	permutation	
대치	substitution	• 평문의 **각 문자를 새로운 문자로 대치**하는 방식 • 환자(換字) 또는 치환라고도 한다. • 예 : 123 → ABC

① 전치와 순열은 같은 개념이다.

• 상황에 따라 전치 또는 순열이라고 기술할 뿐이다.

• 순열(permutation)은 전치 원리이다. 순열은 대치 원리가 아니다.

② 그런데, 순열(permutation)을 치환으로 해석하는 책도 있다. – 주의할 것!

• 예를 들면, permutation table을 순열표라 하지 않고, **치환표**라고 한다.

• 대치를 치환라고도 한다. 따라서 치환표라고 하면 대치 원리를 생각할 수 있다.

• 여러 암호 관련 교재에서 용어 사용에 따른 차이로 혼돈되는 일이 없어야 한다.

탐구

8비트 현대 대칭키 블록 암호에서
암호문의 1의 개수가 3개일 때,
평문을 찾기 위해 필요한 시행착오는 몇 번인가?

◈ **대치암호(substitution cipher)로 암호화가 된 경우 : S-박스**

- 대치암호는 암호문과 평문의 1의 개수가 일치하지 않는다.
- 즉, 평문의 1의 개수가 몇 개인지 알 수 없다.

∴ **시행착오** = 2^8 = **256**(번)

◈ **전치암호(transposition cipher)로 암호화가 된 경우 : P-박스**

- 전치암호는 암호문과 평문의 1의 개수가 일치한다.
- 즉, 평문의 1의 개수는 3개이다.
- 해서, 8비트 블록에서 1의 개수가 3개인 조합의 수를 구하면 된다.

∴ **시행착오** = C(8, 3) = (8 × 7 × 6) / (3 × 2 × 1) = **56**(번)

// 대치암호와 전치암호의 차이점

분석	• 대치암호문을 해독하기 위한 시행착오 횟수가 더 크다.**(256>56)** • 비트 수가 클수록 시행착오 횟수 차이는 매우 커진다.
결론	• 현대블록암호는 대치암호로 설계되어야 안전하다. • 키 크기가 클 경우에 전수조사 공격에 안전성이 보장된다.

// 전치암호, 순열(permutation), P-박스의 관계

[예제] A, B, C – 3개의 문자로 전치 구성 가능한 가짓수

- 가짓수 = P(n, r) = P(3, 3) = 3! = 3 × 2 × 1 = 6(가지) → **순열 이용**
- 순열 집합 = { ABC, ACB, BAC, BCA, CAB, CBA } → 6가지
- 여기서, 순열 집합이 곧 가능한 **전치 종류**가 된다.

기출문제 분석

1. 암·복호화할 때 동일한 키를 사용하는 암호화 알고리즘은? [2015년 국가 7급]

① RSA ② KCDSA
③ SEED ④ ECC

♤ 암호/복호

- 대칭키 암호 알고리즘 : SEED
- 비대칭키 암호 알고리즘 : RSA, KCDSA, ECC

정답 : ③

2. 비대칭키 암호화 알고리즘으로만 묶은 것은? [2017년 지방 9급]

① RSA, ElGamal ② DES, AES
③ RC5, Skipjack ④ 3DES, ECC

♤ 암호 알고리즘 종류

- 비대칭키 알고리즘 : RSA, Rabin, ElGamal, ECC, DSA, KCDSA, ECDSA 등

정답 : ①

3. 다음 대칭키 암호화에서 K값은? [2017년 국가 7급]

○ 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 Q라 함
○ P = 11010011
○ Q = 10000110
---

① 11010011 ② 10000110
③ 01010101 ④ 01010100

♤ 대칭키 암호화

- 다음처럼 구하면 된다.(xor 연산은 같으면 0, 다르면 1)

```
    1101 0011 → P
xor )1000 0110 → Q
    0101 0101 → K
```

정답 : ③

4. 암호 알고리즘에 대한 설명으로 옳지 않은 것은? [2022년 국가 9급]

① 일반적으로 대칭키 암호 알고리즘은 비대칭키 암호 알고리즘에 비하여 빠르다.
② 대칭키 암호 알고리즘에는 Diffie-Hellman 알고리즘이 있다.
③ 비대칭키 암호 알고리즘에는 타원곡선암호 알고리즘이 있다.
④ 인증서는 비대칭키 암호 알고리즘에서 사용하는 공개키 정보를 포함하고 있다.

♤ **암호 알고리즘**

· **대칭키 암호** 알고리즘에는 Diffie-Hellman 알고리즘이 있다.**(×)**
→ Diffie-Hellman 알고리즘은 **키 교환** 알고리즘이다.

알고리즘	수학적 계산	보안성 근거	키 교환	암호/복호	전자서명
Diffie-Hellman 키 교환	지수 합동	이산대수 문제	가능	불가능	불가능
RSA	지수 합동	소인수분해 문제	가능		
Rabin	이차 합동	소인수분해 문제			
ElGamal	지수 합동	이산대수 문제			
타원곡선	타원곡선 (3차방정식)	타원곡선 이산대수 문제			

• 디피-헬만 키 교환은 암호학적 통신 방법의 기초를 수립하였다.
• 디피-헬만 키 교환은 KDC 없이 비밀키(대칭키)를 교환하는 하나의 방법이다.
• 송수신자는 공개된 통신망에서 공통의 비밀키를 생성하여 공유할 수 있다.

정답 : ②

5. 암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키를 사용하는 것은? [2021년 지방 9급]

① SEED ② ECC
③ AES ④ IDEA

♤ **암호 알고리즘**

• 대칭키 암호 : SEED, AES, IDEA, DES, ARIA, HIGHT 등 → **동일한 키** 사용
• 공개키 암호 : ECC, RSA, Rabin, ElGamal 등 → **서로 다른 키** 사용

정답 : ②

6. 다음 중 대칭키 암호화 기법이 아닌 것은? [2022년 군무원 7급]

① RC4 ② ElGamal ③ LEA ④ ARIA

♤ **암호 기법**

대칭키 암호	· 키 교환의 어려움 · 대칭키 암호는 공개키 암호에 비해 처리속도가 빠르다. · DES, SEED, AES, LEA, ARIA, HIGHT, IDEA, RC4, SkipJack
비대칭키 암호	· 대칭키를 교환하기 전에 대칭키 암호회에 이용된다. · RSA, Rabin, ElGamal, ECC, DSA, KCDSA, ECDSA **(공개키 암호)**
해시함수	· 메시지 무결성 제공한다. · MD5, HAS-160, SHA-1, SHA-2, WHIRLPOOL(월풀)

정답 : ②

7. 다음 중 대칭키와 비대칭키에 대한 설명으로 가장 옳은 것은? [2022년 군무원 9급]

① 대칭키 : 빠른 처리 속도
비대칭키 : 키 교환의 장점
② 대칭키 : 암호화 및 복호화 키가 같음
비대칭키 : 3개 이상의 키가 필요
③ 대칭키 : 키 교환의 어려움
비대칭키 : MD5(Message-Digest5) 알고리즘
④ 대칭키 : DES(Data Encryption Standard) 알고리즘
비대칭키 : 개인키 및 공개키 모두 공개

♤ **암호 알고리즘**

대칭키 암호	· 키 교환의 어려움 · 대칭키 암호는 공개키 암호에 비해 처리속도가 빠르다. · DES, SEED, AES, ARIA, HIGHT, IDEA, RC4, SkipJack
비대칭키 암호	· **전자서명**에 사용된다. · 대칭키를 교환하기 전에 대칭키 암호회에 이용된다. · RSA, Rabin, ElGamal, ECC, DSA, KCDSA, ECDSA **(공개키 암호)**
해시함수	· 메시지 **무결성** 제공한다. · MD5, HAS-160, SHA-1, SHA-2, WHIRLPOOL(월풀)

정답 : ①